volume seven | edition one

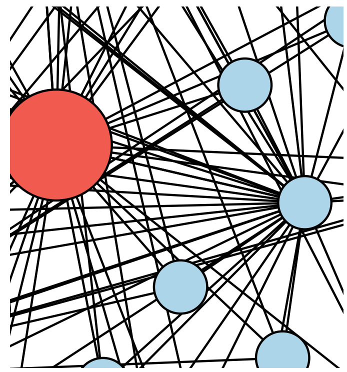
spring 2011

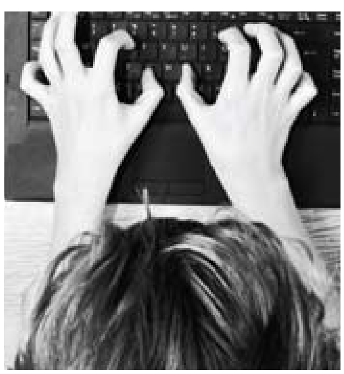
CONSUMER CONNECTION

Arm yourself: Fight fraud. Resist scams. Combat abuse.

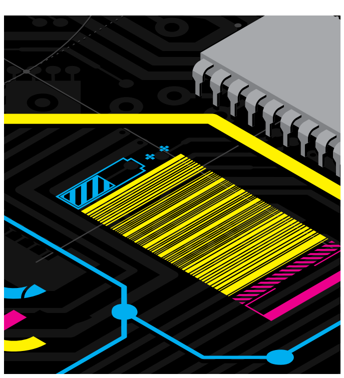
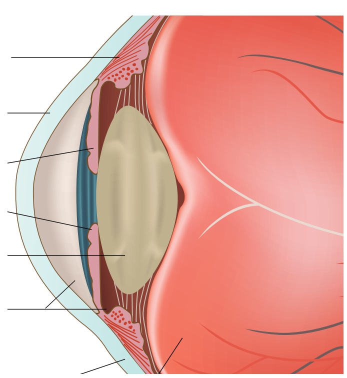







dca

CONSUMER CONNECTION is produced by the Department of Consumer Affairs' Office of Publications, Design & Editing. If you have any questions or comments, please e mail us at consumerconnection@dca.ca.gov.

from the acting director

The Federal Trade Commission, the Consumer Product Safety Commission, and a host of other public and private entities recently observed National Consumer Protection Week. The annual campaign encourages consumers to take full advantage of their consumer rights and make better, more-informed decisions.

A special Web site, **www.ncpw.gov**, has a wealth of advice from Federal and State government entities and partner nonprofit organizations. The site includes tips on how to protect your privacy, manage your money, and steer clear of scams and fraud.

This edition of *Consumer Connection* echoes that mission.

Here's a look at some of the articles in this special consumer protection issue.

Many Californians have seen their finances take a beating over the last few years. As a result, companies involved in debt collection have boomed and so have complaints about some of their practices. The best protection against the abuse by a debt collector is to know your rights as a consumer and to exercise them. We have some tips on how to do that.

Online shopping is a convenience many of us enjoy. However, there are ways we can be taken advantage of while shopping online, especially with the "free trial offer" that can end up being anything but free.

Speaking of online activities, are you aware that the Web sites you visit and the links you click on may be tracked by third-party companies without your knowledge? Government officials have started talking about the need for "do-not-track" regulations to ensure privacy online. In the meantime, some of the most-popular Web browsers are adding their own do-not-track options that consumers can download.

New government regulations are helping consumers be more informed about their credit scores. Under new Federal rules, consumers must be given more information about how their credit scores impact a lender's decision to grant them credit.

DCA recently unveiled an online self-help tool to guide users to resources on just about any topic of interest to consumers. The new Consumer Wiki is based on the open-source software used in the popular Wikipedia.

In addition, one of our most popular publications, *Department of Consumer Affairs: Who We Are and What We Do*, has been updated for 2011. The booklet contains a list of the professions and occupations licensed and regulated by the Department and guidance on how to contact us for more information, to verify a license, or file a complaint.

As always, consumers can call DCA's Consumer Information Center toll-free at 800.952.5210 for information and assistance. We look forward to hearing from you.

Brian J. Stiger

BRIAN J. STIGER, Acting Director
California Department of Consumer Affairs

what to do if the debt COLLECTOR calls

It's no secret that the finances of many people have taken a beating over the last few years. This led to an increase in consumers who are unable or unwilling to pay their debts. This has created a boon for debt collectors.

In a 2009 survey conducted by the Pew Research Center for the People of the Press, 21 percent of respondents reported they'd had problems with collection or credit agencies over the past year. It can happen to anybody, and there is no "typical" debtor, according to ACA International, a worldwide association that represents debt collection companies.

Debt problems can stem from poor money management skills, job loss, prolonged illness, or a multitude of other circumstances. Most accounts are referred for collection because they have gone unpaid for several months and the creditor has not received communication from the consumer, says ACA.

If you fall into that group somehow, here's what you do:

step one

Don't panic. You have rights.

Debt collection companies in California are regulated by the Fair Debt Collection Practices Act (FDCPA), which is administered by the Federal Trade Commission (FTC), as well as California's Rosenthal Fair Debt Collection Practices Act (Civil Code 1788-1788). The primary difference is the Federal law applies only to third-party debt collectors, while the Rosenthal Act covers original creditors as well.

The FDCPA is designed to protect consumers from abusive, misleading, and unfair debt collection practices, and it gives debtors specific protections. These include the right to cut off contacts by a debt collection agency; the right to specify when and how you can be contacted (for example, in writing only); and the right to dispute a debt.

step two

Don't hide.

The most important thing you can do if you receive a demand for payment is to respond immediately, both by telephone and in writing. The faster you and the collector communicate, the quicker the matter can be resolved. Next, call DCA's Office of Publications, Design & Editing 866.320.8652 for a free copy of *What to Do If You Receive a Demand for Payment from a Creditor or Debt Collection Agency* (also called "Legal Guide DC-1"). You can also find it online at **www.dca.ca.gov**. Click the "Publications" tab, then the "Legal Guides" link.

This is also critical: If you receive a court summons regarding a debt, show up. Bring copies of any payment receipts, contracts, collector communication, and anything you have to support your case. Failure to appear in court can, and often does, result in a default judgement against you.

The FDCPA requires third-party collection agencies to provide a written notice with the debt amount and the name of the creditor to whom the debt is owed within five days after its initial communication with you about it, but the law gives you the right to ask for even more information including the name and address of the original creditor, if different from the current one. You have to make this request within 30 days after you receive the first collection notice. Remember: Any communication you have with the collector should be in writing.

BEFORE YOU agree to PAY, consider this:
DO you REALLY OWE the MONEY?

Be aware that some collectors try to intimidate consumers into paying debts they don't actually owe.

The debt may not be legally collectible for any of following reasons:

- The debt is owed by someone else, not you (though you may be liable if you co-signed for it).
- The debt is too old to be legally enforceable (the statute of limitations has passed). However, if you make a payment, enter into a payment plan, make an agreement to pay, or charge against the account, by law, the statute of limitations starts over.
- The claim is based on an agreement that must be in writing, but there is no written contract.
- You were billed for an item that you never ordered.
- You were billed for an item that you ordered but never received.
- You returned an item, but you were billed for it anyway.
- The contract is one that you have a right to cancel, and you properly cancelled it, or can still cancel it.
- You are a victim of a fraud, and the contract or sale is therefore void or voidable.
- The debt has been discharged in bankruptcy.

You may need to consult an attorney to help you determine if you legally owe the debt. Find a lawyer by contacting your Employee Assistance Program or through the State Bar of California's Lawyer Referral Services Program at 866.442.2529 or 866.44.CA.LAW.

You can also visit your local legal aid society or legal assistance office (check the white pages of your phone book) or self-help legal sites such as Nolo.com (try **www.nolo.com/legal-encyclopedia/collection-agencies/**) or **www.LawHelpCalifornia.org**. In addition, the California Courts Online Self-Help Center, sponsored by the Judicial Council of California, has a list of resources on free and low-cost legal help.

If you do owe the money, or a portion of it, work with the collection agency to pay it off. You can request an installment plan if that helps you, but the collector doesn't have to agree to it, and can demand payment in full. Make sure to get any payment agreement in writing.

But even if you do owe money, you don't have to stand for abuse, harassment, or intimidation from a debt collector.

The *Ventura County Star* reported that Californians have filed more than 40,000 complaints with the FTC against debt collectors since 2007, according to an analysis of Federal data. A new cottage industry of debt buying has transformed the credit and collection industry. In the last decade, the buying and selling of debt portfolios for pennies on the dollar has been common. The owners of these debt portfolios often don't have sufficient documentation to substantiate the amount owed, and may not even have the correct debtor, according to a 2011 report by the California Department of Consumer Affairs. Buyers of debt portfolios directly file court actions, overwhelm the court system, and almost always obtain a default judgment. Many of these alleged debtors claim they were never properly served notice and didn't know about the debt until they learned of the default judgment, which can be emotionally and financially devastating.

While there are many hardworking, honest collectors, some use unscrupulous tactics. While few would argue that consumers should be responsible for their debt, collection industry representatives are responsible for using lawful remedies to collect it.

In fact, ACA requires companies to adhere to a code of ethics and operations as a condition of membership, which includes language requiring members to "maintain the highest standards of business conduct by using only legal and ethical means in all business activity."

ANY COMMUNICATION you have with a DEBT COLLECTOR should be in WRITING.

What collectors can't do

State and Federal law prohibits debt collectors from certain activities. They cannot:

- Use, or threaten to use, physical force or violence or any criminal means to harm you, your reputation, or your property.
- Communicate with your employer about the debt (without your written permission) except to call and confirm you work there.
- Use obscene or profane language.

- Threaten any action that they don't intend to take, or is against the law.
- Call you before 8 a.m. or after 9 p.m.
- Cause a telephone to ring repeatedly, or contact you so often it constitutes harassment.
- Discuss your debt with anyone else.

What collectors can do

Believe it or not, we all benefit from legitimate collection activity, according to a national study by global advisory firm PricewaterhouseCoopers. Debt collectors return more than $40 billion per year to the U.S. economy, helping businesses keep prices down and saving the average American family $354. This amount represents dollars households would have spent if businesses were forced to raise prices to cover bad debt. Collection agencies are legitimate businesses, and the laws permit certain activities to help them do their job. They are allowed to:

- Contact another person to confirm your location or enforce a judgment.
- Sue you in Superior Court if you ignore their collection attempts, get a court judgment against you, and use it to garnish your wages.
- Add interest to the debt owed, although within limits specified by the agreement that created the original debt, or by law. Ask the collection agency in writing to explain to you—also in writing—how much interest is added and why.

But many consumer advocates believe these rules don't go far enough. In a 2010 report, the FTC noted that it receives more complaints about the debt collection industry than any other. Third-party collectors contact millions of consumers each year: Because of the sheer numbers, chances are you or someone you know has been one of them.

What if I'm an identity theft victim?

You're not alone. There were 11.1 million U.S. residents who were victims of identity theft in 2009, according to the California Office of Privacy Protection. The State's Rosenthal Act has specific protections for you. If you've been a victim of identity theft, and you get a call from a collector on a resulting debt, do the following as soon as possible:

Send the collection agency a copy—by certified mail—of the police report you filed for the identity theft crime. Provide a written statement saying you believe you've been a victim of identity theft with respect to the specific debt. Include a completed copy of the FTC's "Identity Theft Victim's Complaint and Affidavit." Follow the "Identity Theft Victim Checklist" on the California Office of Privacy Protection's Web site (**www.privacyprotection.ca.gov** under the "Identity Theft Resources" heading) or call 866.785.9663.

If you simply told the collector that your identity was stolen, the Act requires the collector to tell you that you must provide written notice.

Other tips and how to complain

Visit the California State Attorney General's Web site for guidelines on what collectors are allowed to do at **ag.ca.gov/consumers/general/collection_agencies10.php**. Also review *Debt Collection FAQs: A Guide for Consumers* on the FTC's Web site (look under the "Debt Collection" link on the home page).

If you think a debt collector has violated a law, you can file a complaint with the California Attorney General's Office 800.952.5225 as well as the FTC at 877.FTC.HELP or 877.382.4358. Collection laws give you the right to sue a collector in a State or Federal court within one year from the date of the violation.

What's being done to thwart debt collection abuses?

In 2010, DCA hosted six consumer protection roundtable meetings across California with State and Federal agencies, nonprofits, law enforcement prosecutors, Legislative staff, and academics. These consumer leaders reported on issues of interest to their constituents, and complaints about harassing and litigious debt collection practices were a common theme. This led to two more meetings specifically devoted to debt collection practices. The consensus was that legislation and additional regulations are needed in California to bolster protection for consumers.

Federal legislation may help. The "End Debt Collector Abuse Act of 2010 (S.3888)," introduced in September 2010 by Senator Al Franken of Minnesota and Senator George LeMieux of Florida, sought to amend the FDCPA and provide stricter regulations for the debt collection industry. If passed, it would have required better disclosure about the debt details, increased penalties for consumer rights violations, and perhaps most importantly, prohibited collection agencies from obtaining arrest warrants. Although the Congressional session ended before it could be voted on, the authors vow to revive it soon.

While many industry representatives are honest and follow the rules, many don't. Consumer advocates, including the FTC, agree that more public education is needed so consumers understand their rights, and realize that what may seem like harassment or annoyances are actually legitimate collection activities. But until stiffer penalties make it on the books, it's up to take-charge Californians to learn their rights to avoid adverse consequences and financial pain.

HOW TO RESPOND [in writing] to a debt collector

You can use the letter below, or a similar one, to notify a collection agency that you do not wish to be contacted. Note that this will not stop further debt collection actions such as lawsuits, repossessions, or wage garnishments, but it will stop further contact. Be sure to send the letter via certified mail, return receipt requested—and to keep a copy.

Also note that this applies only to third-party debt collectors—primarily collection agencies—not to the primary creditor.

> [Date]
>
> [Collection Agency Name]
> [Address]
> [City] [State] [Zip]
>
> To Whom It May Concern:
>
> In Re: [Name or names on account]
> [Account number]
> [Name of creditor]
>
> Since [date], I have been receiving telephone calls [at home and/or at my place of employment] from you concerning my account with the above-named creditor.
>
> This letter is to inform you that, pursuant to the provisions of the Fair Debt Collection Practices Act (15 U.S.C. §1692c), I am requesting that you cease all further communications with me except to the extent specifically permitted under law.
>
> Very truly yours,
>
> [signature]
>
> [Your name printed or typed]
> [Your address]
> [Your city, state, zip]
> [Your telephone number]

Source: ConsumerAffairs.com

TIME FOR A NEW ROOF?

You wouldn't go outside during a rainstorm without an umbrella, right? The roof on your house is its umbrella. It protects the inside of your home and many valuable contents from potential damaging effects of the weather, especially rain and snow.

A leaky roof will allow water to come inside and eventually ruin walls and insulation and collapse ceilings. It could also put your family at risk by short-circuiting wiring, which can cause an electrical fire.

The first sign of a leaky roof often appears when interior walls or ceilings show water stains.

The first sign of a leaky roof often appears when interior walls or ceilings show water stains. Before you blame the roof, make sure the leak isn't coming from faulty water pipes in the attic. Finding the source of a leaky roof can be tricky because water entering through the roof can run a good distance before pooling up and dripping into the house.

Consider hiring a professional to determine the source of the leak and provide options on how to make repairs. The average life expectancy of a residential roof is between 15 and 20 years. Replacement factors include the age and condition of the existing roof as well as the severity of weather in your area.

Hiring a contractor

The best way to find a qualified roof contractor is to contact friends or neighbors who have had a roof repaired or replaced recently. Ask if they were satisfied with the quality of the materials and craftsmanship, the time it took to complete the job, and the integrity of the contractor. Be sure to get three estimates and compare each one as prices between contractors can vary significantly. Be sure to work only with contractors who are licensed through the Contractors State License Board. To verify a license, go online to **www.cslb.ca.gov** or call the Board at 800.321.CSLB or 800.321.2752.

The contract

Do not allow work to begin until after you have a signed contract. The contract should include the price; details of the work performed; the type of material being used; removal of all construction debris; and expected start and completion dates. If you see any terminology in the contact you don't understand, ask for an explanation. Don't sign on the dotted line until you understand all aspects of the contract.

After you chose a contractor to perform the work, the law permits the contractor to request no more than 10 percent of the total cost or $1,000, whichever is less. Final payment should not be made until all the work is complete and you are satisfied. Be sure the contractor obtains all the necessary permits required by local building codes before work begins.

Have the contractor show proof that he or she carries workers compensation and general liability insurance. Finally, protect yourself from a mechanic's lien if for some reason the contractor fails to pay subcontractor or material suppliers. Ask for a "release of lien" clause in the contract.

The Contractors State Licensing Board has a brochure titled *Tips for Hiring a Roofing Contractor*. It contains tips on roof maintenance and hiring/dealing with roof contractors, managing problems, and more. View a copy online at **www.cslb.ca.gov** or call the Board at 800.321.CSLB or 800.321.2752 to have a copy mailed to you at no charge. The material is also available in Spanish.

Other considerations

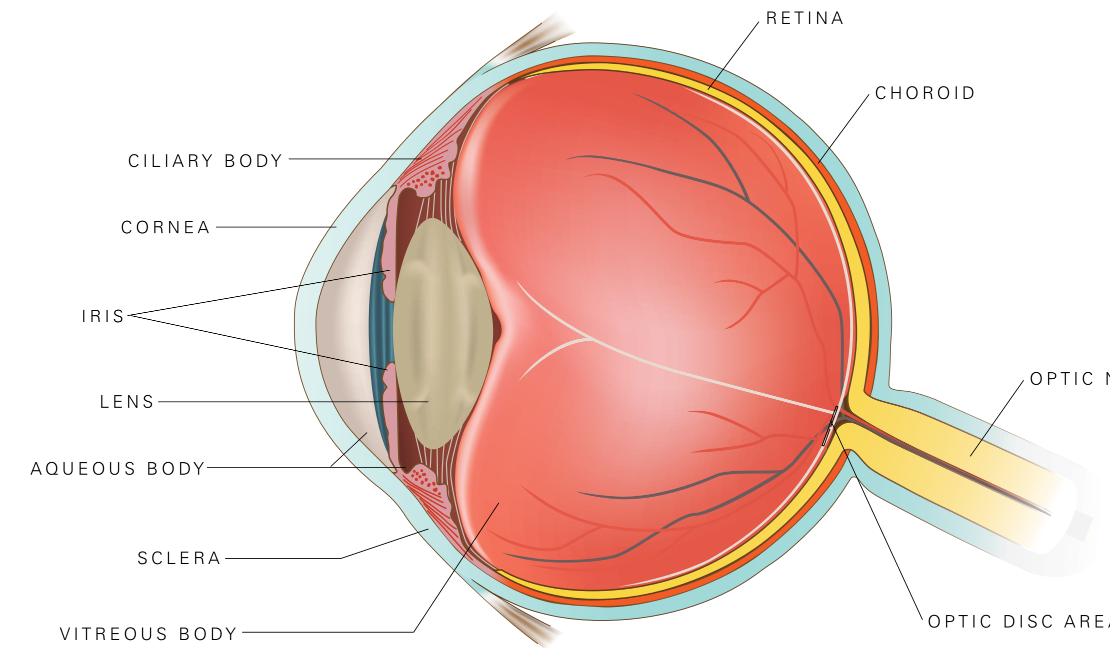
If you've had roof leaks before, it's best the have all layers of shingles removed down to the plywood sub-roof. This allows the contractor to examine the structure of the roof before installing new shingles. A common problem is roof rot of the plywood sheathing under the shingles. This wood decays over time from exposure to heat and humidity. Fixing roof rot is critical prior to installing new shingles. Metal flashing should also be inspected or replaced around venting pipes, exhaust fans and roof vents to ensure a water-tight seal.

The contractor should provide one price to strip off the old shingles, repair/replace roof vents and flashing, install the new roof and finally remove all old material and debris. Keep in mind that roof rot repair will probably not be included in your original estimate since the contractor won't know the extent of the damage and cost of repair until all the old shingles are removed.

This is also a good time to inspect the condition of your gutters and downspouts. Many roofers also install gutters, so consider replacing them at the same time.

The benefit

A new roof is a long-term investment that will help protect your possessions and keep your family safe. Don't wait for serious problems to begin before you repair or replace it with a new one.



New law allows optometrists to treat glaucoma

If you have glaucoma, or are at risk for it, you have another option for treatment, under a new State law. Under Senate Bill 1406, optometrists licensed in California can become certified to manage and treat glaucoma patients without consulting an ophthalmologist. The law was signed by Governor Arnold Schwarzenegger in September 2008; regulations implementing it became effective January 8, 2011.

Before the new law passed, optometrists could screen patients for glaucoma, but had to refer them to an ophthalmologist (a medical doctor who specializes in diseases and conditions of the eye) for treatment.

According to a report commissioned by DCA's Office of Professional Examination Services, this change puts California in line with every state in the nation except Massachusetts in allowing glaucoma treatment by optometrists.

Glaucoma, the second leading cause of blindness in the United States, cannot be cured, although it can be controlled with prescription eye drops or with surgery, according to the American Health Assistance Foundation (**www.ahaf.org**). According to the Foundation, many people do not realize they have glaucoma until they experience vision loss, which is permanent. The condition affects all age groups, but is more common in people over 60. Early detection and treatment are key to preserving eyesight.

Supporters of the new law say it will bring greater access to glaucoma care to all Californians, especially those in areas of the State without ophthalmologists. There are about 7,000 actively licensed optometrists in California, and fewer than 3,000 ophthalmologists, according to the DCA report. In some parts of the State, optometrists are the only eye care professionals nearby.

California-licensed optometrists who wish to treat glaucoma patients must be certified by the Board of Optometry to do so. Optometrists who graduated from an accredited school of optometry after May 1, 2008, can become certified without additional training. Optometrists who graduated before that date must take 24 hours of specialized training, plus meet other requirements. There will also be continuing education requirements. The Board of Optometry will not accept glaucoma certification from another state.

Even with certification, there will be limits to what an optometrist can do. Some patients may still be referred to an ophthalmologist for treatment. To learn more about glaucoma certification for optometrists, visit the Board of Optometry online at **www.optometry.ca.gov** or call the Board at 866.585.2666.

When conducting business online, you can’t be too careful.

PLAY YOUR CARDS right FOR SECURE SHOPPING

One trick that consumers are often duped by is the "free trial offer." What happens when the trial period ends, but charges mysteriously continue? The Federal Trade Commission says if you see a free trial offer online for a product you're interested in, stop and read the details:

READ THE TERMS AND CONDITIONS. If you can't, or don't understand them, look for another merchant. You don't want to commit to recurring charges for products or services by mistake—or before you've tried them and made your decision.

LOOK FOR PRE-CHECKED BOXES. That check may bind you to terms and conditions you're not comfortable with or ready to accept.

LOOK FOR INFORMATION ABOUT HOW TO CANCEL future product shipments or services if you don't want them. Do you have to pay? Do you have a limited time to respond?

READ YOUR CREDIT AND DEBIT CARD STATEMENTS right after you've responded to a free trial offer—and often afterward—looking for charges you don't recognize or didn't authorize. Contact the merchant first to try to resolve any issues, but notify the card issuer promptly if you don't recognize a charge.

For added safety, stick to reputable sites, says **CreditCards.com**—it's easy for scammers to set up fake Web sites and lure you in with super-low (and also fake) prices. And don't buy anything from someone soliciting you via e-mail.

Another way to protect yourself is by using reloadable debit cards. You prepay with cash, the amount is loaded on the card, and you can use it almost anywhere you could use a traditional debit or credit card, including online. If the card should fall into the wrong hands, your risk is limited only to the amount you put on the card.

Also remember when shopping online and elsewhere that credit cards offer more protections than debit cards. For example, you can always dispute a fraudulent charge on a credit card, but if a thief gets your debit card and uses it, the money comes out of your checking account immediately. It can take a lot of paperwork, time, and frustration to get your bank to reimburse you, if it does at all. Meanwhile, you're out the money. Check your account terms and conditions: Some companies impose a deadline for alerting the bank to suspected fraudulent activity.

Finally, follow these tips from the California Office of Privacy Protection:

PROTECT YOUR SOCIAL SECURITY NUMBER. Don't carry your card with you. Keep it in a safe place at home. A thief can use it to open up accounts in your name and start spending.

INSTALL PROTECTIVE SOFTWARE ON YOUR COMPUTER and keep it updated. Avoid free downloads that may carry spyware capable of stealing personal information from your computer.

NEVER CLICK ON LINKS IN E-MAILS FROM ANYONE YOU DON'T KNOW, and be extra cautious even if you do. For example, that e-mail that appears to be from your bank alerting you to some account problem is likely a phishing message designed to steal your information. Pick up the phone and call your bank if you're concerned.

CONTROL YOUR PERSONAL INFORMATION. Ask questions whenever you are asked for details that seem inappropriate for the transaction. (For example, why would your bank account information be needed for a "free trial offer?") Ask how the information will be used, if it will be shared, and how it will be protected. If you're not satisfied with the answers, cancel the transaction.

Learn more at www.privacy.ca.gov.

DCA: A friend in the marketplace

Does that contractor you hired to redo your bathroom have proper insurance in case an employee is injured on the job? Is your nail salon following lawful procedures to protect you from infection? Think you might be driving a lemon? These are just some of the questions the California Department of Consumer Affairs (DCA) can help you answer.

No matter what consumer problem faces you, chances are there's a DCA program that can help you solve it. Not sure who to call? Request a copy of our newly updated booklet, *Department of Consumer Affairs: Who We Are and What We Do*, by calling DCA's Office of Publications, Design & Editing toll-free at 866.320.8652. In the booklet, you'll find contact information for all of our consumer regulation entities, along with tips to protect yourself from unscrupulous operators. Keep it handy for easy access anytime you have a consumer problem.

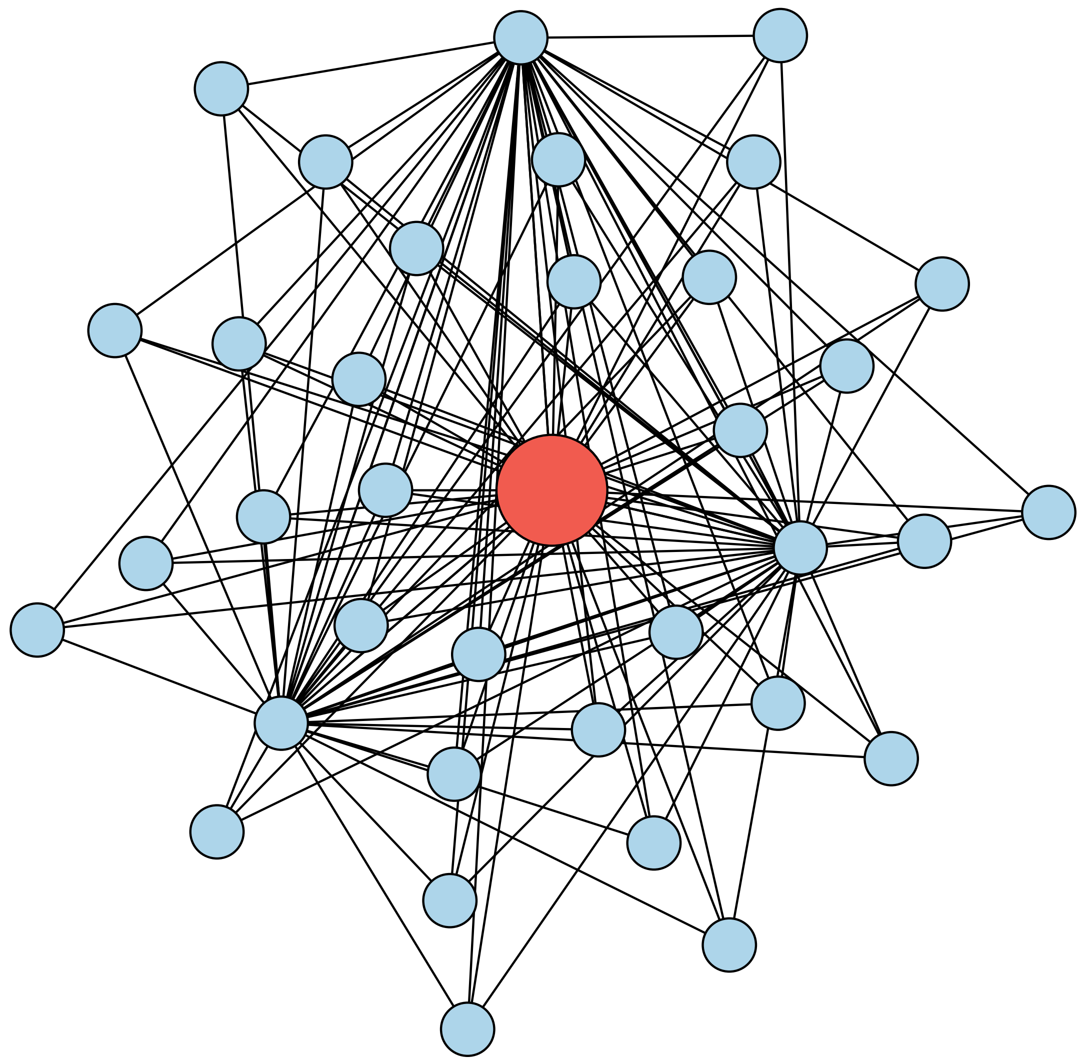
DCA supports consumers

All of us buy services from professionals such as accountants, doctors, cosmetologists, and many others. The marketplace, where these transactions happen, is as old as civilization itself. Equally ancient are the practices of fraud and cheating. The Department of Consumer Affairs protects the rights of both buyers and sellers to help ensure a fair marketplace.

Through our boards, bureaus, commissions, and programs, we:

- Advocate consumer interests before lawmakers.
- Ensure minimum competency levels, and only license professionals who pass specialized examinations and meet experience and training requirements.
- Investigate complaints and discipline violators.
- Work with the California Attorney General's Office and local district attorneys' offices to fight fraud in the marketplace.
- Provide current license status information on more than 2.5 million professionals in 240 occupational categories.
- Mediate disputes between businesses and consumers.
- Bring information directly to consumers through community presentations and events, and by developing partnerships with city, county, state, and local consumer protection leaders.

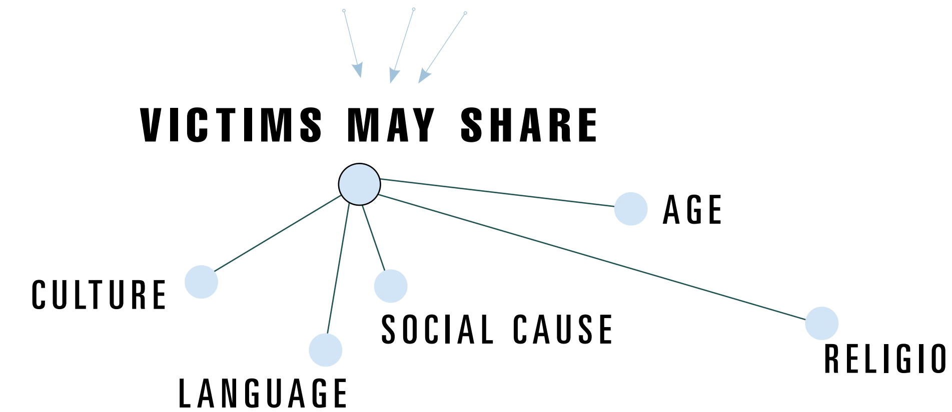
When it comes to navigating the marketplace, you're not alone. If you experience any kind of consumer problem, call our Consumer Information Center toll-free at 800.952.5210, visit **www.takecharge.ca.gov**, or e-mail us at **dca@dca.ca.gov** or **TakeChargeCA@dca.ca.gov**. You can also access our consumer self-help directory from the DCA home page, **www.dca.ca.gov**, or directly at **consumerwiki.dca.ca.gov**.



affinity fraud

HOW SCAM ARTISTS FIND VICTIMS IN GROUPS

IT'S A RUSE THAT RELIES ON CONNECTIONS



It happens to people with ties, people who share an age group, a culture, a language, a religion, a social cause. Because of that, they trusted the person in their group who came to them asking for money. Maybe the person cited Bible verses, or talked about helping those left behind, or just reaping the rewards of a lifetime of hard work. A church minister, a community elder, or a respected authority figure may have vouched for the person. The investment sounded good, and they saw no reason to doubt the person's honesty.

That's the tale told by thousands of trusting people nationwide—members of ethnic groups, religious groups, cultural, or community organizations who willingly ponied up thousands of dollars, sometimes a life savings, to con artists who used the money to fund a lavish lifestyle, or who simply collected the cash and vanished. And when the scam was eventually revealed to the stunned investors, the most common reaction was: It can't be true; he (or she) was one of us.

It's called affinity fraud, and the con artists who practice it take time to build a network of trust (an affinity) with members of a group. When presented with an investment opportunity, the natural skepticism of an individual is overcome by the group dynamic. The more tightly knit the group, the stronger the group dynamic. Group loyalty and the desire to be accepted takes over, drowning out the skeptics. When that happens, the scam artist has won.

Many affinity scams involve "Ponzi" or pyramid schemes, according to the U.S. Securities and Exchange Commission. Under a Ponzi or pyramid scheme, money from new investors is used to pay dividends to earlier investors. The early payments generate testimonials, giving the false impression that the investment is paying off. However, the scheme depends on an unending supply of new contributors. When the supply dries up, the scheme collapses. The Bernie Madoff case is a recent example of a high-level Ponzi scheme. His scheme also had elements of an affinity fraud. Many of the victims were wealthy people in his social and religious circle. Their losses totaled $50 billion.

The FBI has reported a steady increase in investment fraud over the past few years, particularly in Ponzi and market manipulation schemes. Operation Broken Trust, a Federal government task force, was created in 2009 to investigate and prosecute investment fraud. Affinity fraud was only one of the areas covered. Other areas included mortgage scams, tax fraud, predatory lending, credit card fraud, and other financial crimes.

The task force was aptly named. Consumer advocates say affinity fraud takes an emotional toll on its victims in addition to a financial toll. The betrayal of trust can be devastating. Victims can even be in denial that they were taken. Many times, victims try to settle the matter within the group instead of involving law enforcement. That's part of the reason that only very widespread cases ever reach the attention of local police or Federal authorities, experts say.

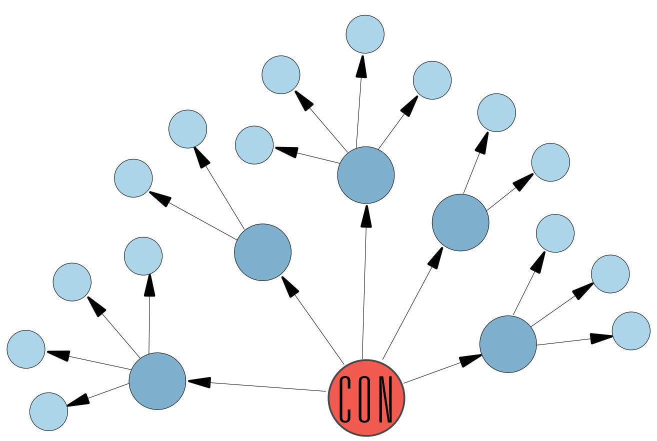
The Operation Broken Trust sweep ended in December 2010. The result: Charges filed in 211 cases with more than 120,000 victims who lost a combined $8.3 billion. In a press release announcing the result of the three-and-a-half-month sweep, Attorney General Eric Holder called the victims' losses "staggering," adding, "These losses represent hard-earned money and even life savings. They represent needs that may not be met and dreams that may not be fulfilled. All of these victims can tell a tragic and cautionary story of being misled and exploited—often by someone they trusted.

"In fact, many of the scam artists we've identified were preying on their own neighbors—and on the most vulnerable members of their communities," Holder said. "Several of those prosecuted during this operation solicited victim investors from their own churches. One man in Texas allegedly targeted his fellow parishioners, asking them to invest with him and claiming that his success in foreign exchange trading was 'a blessing from God.'"

IN ONE SCHEME a con artist PROMISES PEOPLE LARGE PROFITS for bringing others INTO THE PROGRAM

In some cases associated with religious groups, con artists told the potential victims that investments tied to church groups were not subject to Federal securities laws. That is not true. Virtually all investment opportunities, including church bonds, are subject to Federal and State securities and commodities laws. A person must be licensed to sell them.

Affinity fraud, also called a crime of persuasion, doesn't always involve bogus investments. It can be as innocent-sounding as a gifting or dinner party (online or in person). You have to pay money and bring in more members (who also pay money) before



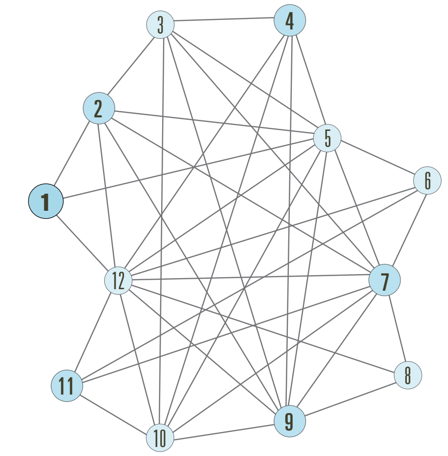
you can make money. Scam artists frequently pay out "dividends" to early joiners to build enthusiasm. How do you know it's a scheme? One way to tell is that the promoters promise large profits simply by bringing other people into the program. In a pyramid scheme, the program may include a product to sell, although very few sales actually take place. In reality, investors are the only source of funding.

Members of the California Consumer Affairs Association addressed the problem of affinity fraud as part of their annual conference held in November at the Department of Consumer Affairs in Sacramento. A panel of consumer advocates recommended enhanced consumer education (in various languages) as one way to help keep people from becoming victims. The speakers also urged consumers to contact the authorities if they suspect fraud. It's important to realize, however, that even if a con artist is arrested and convicted, the victims may never get their money back.

HERE ARE some red flags suggesting an investment opportunity may be a fraud:

- **High investment returns with little or no risk.**
  Every investment carries some degree of risk, and investments yielding higher returns typically involve more risk. Be highly suspicious of any "guaranteed" investment opportunity.
- **Overly consistent returns.**
  Investments tend to go up and down over time, especially those seeking high returns. Be suspect of an investment that continues to generate regular, positive returns regardless of overall market conditions.
- **Unregistered investments.**
  Ponzi schemes typically involve investments that have not been registered with the SEC or with state regulators. Registration is important because it provides investors with access to key information about the company's management, products, services, and finances.
- **Unlicensed sellers.**
  Federal and state securities laws require investment professionals and their firms to be licensed or registered. Most Ponzi schemes involve unlicensed individuals or unregistered firms.
- **Secretive and/or complex strategies.**
  Avoiding investments you don't understand or for which you can't get complete information is a good rule of thumb.
- **Issues with paperwork.**
  Ignore excuses regarding why you can't review information about an investment in writing, and always read an investment's prospectus or disclosure statement carefully before you invest. Also, account statement errors may be a sign that funds are not being invested as promised.
- **Difficulty receiving payments.**
  Be suspicious if you don't receive a payment or have difficulty cashing out your investment. Keep in mind that Ponzi scheme promoters sometimes encourage participants to "roll over" promised payments by offering even higher investment returns.

SOURCE
Investor.gov



1 OF THE BEST WAYS to prevent problems IS TO CHECK OUT any investment opportunity THAT COMES TO YOU

HERE ARE some ways to do that:

2 **California Department of Corporations**
The Department regulates broker-dealers, investment advisers, financial planners and others, and regulates the offer and sales of securities, franchises, and off-exchange commodities. The Department's Web site has tools for consumers on how to avoid investment fraud.

3 www.corp.ca.gov
(Click on "Consumer")
866.ASK.CORP or 866.275.2677

4 **Securities and Exchange Commission**
The SEC oversees the key participants in the securities world, including securities exchanges, securities brokers and dealers, investment advisors, and mutual funds.

5 www.sec.gov
(Click on "Investor Education")
800.732.0330

The SEC also maintains an investor-oriented Web site that offers guidance, alerts, and tips on avoiding fraud.

6 www.investor.gov

7 **Financial Fraud Enforcement Task Force**
The task force, which consists of Federal, State, and other entities, works to investigate and prosecute significant financial crimes. The Task Force Web site has information on how to protect yourself from fraud and report problems.

8 www.stopfraud.gov

9 **Federal Trade Commission**
The FTC works to prevent fraud, deception, and unfair competition in the marketplace.

10 www.ftc.gov
(Click on "Consumer Protection")
877.FTC.HELP or 877.382.4357

11 **U.S. Commodities Futures Trading Commission**
The Commission regulates commodity futures and option markets in the United States. Commodity futures and options include precious metals such as gold and silver; foreign currency; crude oil or heating oil; or agricultural products such as corn, soybeans, or cattle.

12 www.cftc.gov
(Click on "Consumer Protection")
866.366.2382

CONSUMER ROUNDUP OF

scams to avoid,

ADVICE TO FOLLOW,

AND

TIPS TO SHARE.

NEW FROM DCA

ONLINE DIRECTORY

answers your questions

Early last December, the Department of Consumer Affairs (DCA) unveiled a new online self-help tool that offers consumers a wealth of information about almost any consumer topic.

The Consumer Wiki (based on the open-source software used in the popular Wikipedia) allows users to look up answers to their questions or find the places to get the answers they need.

“This powerful new tool is the exact same tool used by our call center staff when assisting consumers,” said DCA Acting Director Brian Stiger. “In developing it, we decided to put it out there as a self-help site for consumers to use, too.”

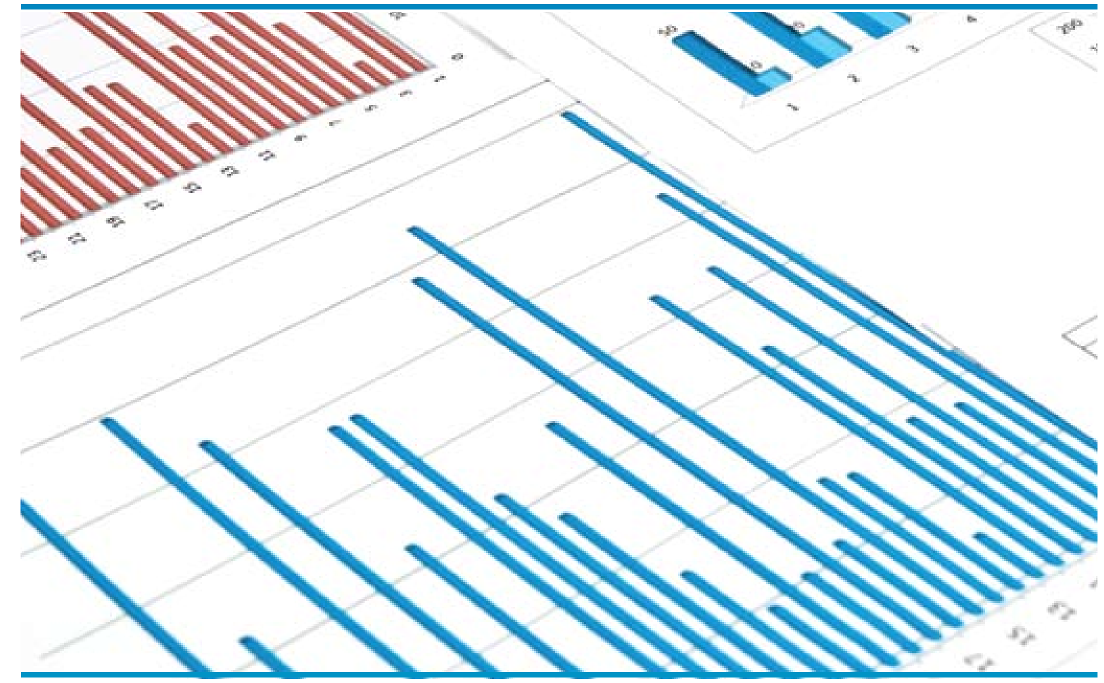
The Consumer Wiki was created to replace an older database of information used by phone agents in DCA’s Consumer Information Center, who handle more than one million consumer calls every year.

Consumers will find valuable information in this directory on thousands of subjects, including contact names and phone numbers for further assistance. Topics range from those consumer issues over which DCA has jurisdiction, such as auto repair and contractors, to other areas such as landlord-tenant issues, buying or selling a home, and financial investments. It includes broad consumer topics as well as an A-to-Z listing of consumer issues.

“We designed this to be easy to update,” said Stiger. “If a consumer finds another resource they think we should include, they can e-mail it to us, we’ll evaluate it and, if appropriate, add it to the site. We want to make this as complete a resource as possible.”

DCA’s Consumer Wiki includes street addresses, e-mail addresses, and phone numbers to government agencies and nonprofit organizations; links to Web sites consumers are likely to want to visit; and a list of DCA publications.

www.consumerwiki.dca.ca.gov



Consumers get more notice about their credit

Beginning this year, consumers who apply for credit will get more information about how their credit report and credit score influences a lender’s decision to grant them credit.

HERE ARE SOME FEATURES OF THE NEW FEDERAL RULES:

Credit score

In some cases, when you apply for a mortgage, an auto loan, or some other type of credit, you will be given a notice that gives your credit score and how that score compares to other consumers’. The notice will also include information on how to get a free copy of your credit report and what to do if you find errors in it.

Risk-based credit

If you are offered loan terms that are less favorable because of information in your credit report, you will be given a risk-based pricing notice. This notice also includes information on how to get a free copy of your credit report and what to do if you find errors in it.

Interest rate hike

If the annual percentage rate on your existing credit account is raised after a review of your credit report, you will receive an account review notice. The notice has information on how to get a copy of your credit report and what to do if you find errors in it.

A new online guide from the Federal Reserve has information about credit reports, credit scores, and the importance of protecting personal credit histories. *The Consumer's Guide to Credit Reports and Credit Scores* describes the content of a credit report, explains how a credit score is used, and discusses the role of credit bureaus in collecting and disseminating this information.

The Consumer's Guide to Credit Reports and Credit Scores can be found at www.federalreserve.gov/creditreports. It is one of several online Federal Reserve publications, such as *5 Tips for Improving Your Credit Score* and *5 Tips for Getting the Most from Your Credit Card*. Many of these publications are available in Spanish.

KINOKI ‘DETOX’ FOOT PADS

KICKED OFF THE SHELF!

You’ve probably seen the television commercial and have seen how convincing the pitch is. The makers claim the foot pads, based on an ancient Japanese “secret,” remove toxins, metabolic wastes, heavy metals, and chemicals from your body. They also claim to treat headaches, depression, insomnia, arthritis, and high blood pressure, just to name a few.

Kinoki Foot Pads sold for $19.95 plus $9.95 for shipping and handling. Do you want to “foot” the bill and purchase a product that makes false and unsupported health benefits? No? The Federal Trade Commission (FTC) doesn’t want you to either.

At the request of the FTC, a Federal judge banned the company from promoting or selling the product. The FTC charged the marketers with running deceptive ads on TV and online with claims that were false and/or unsupported. The owner of the company did not admit to any wrongdoing, but agreed to a $14.5 million dollar judgment, which represents the total revenue from the sale of the foot pads. Payment of the settlement was suspended due to the company’s inability to pay.

ELECTRONIC PICKPOCKET

DOES your credit card or debit card have an RFID logo? If so, it's possible the personal information on that card could be stolen, without the card ever leaving your purse or wallet. Radio Frequency Identification (RFID) is a technology that uses radio waves to transmit information from a chip-embedded card to a portable reading device.

The first use of RFID technology began with security badges for entry into office buildings, apartments, condos, and parking garages. Passports have them and this technology is even being considered for use in California driver licenses. Recently, the financial services industry began to embed RFID chips on credit and debit cards, like the MasterCard "PayPass."

To pay for an item using the MasterCard "PayPass," you simply tap your card on a reading device at the convenience store, gas station, coffee house, or fast food restaurant. It makes payment fast and easy. No need to provide identification or your signature. All of this is good for convenience and speed. Unfortunately, there is a down side.

Skimmers armed with RFID equipment go into nightclubs, shopping malls, and sports arenas with a reading device disguised as a day-planner or small canvas notebook. Simply by getting close to your purse or wallet, they are able to scan the information from your card. Once they have your name and credit card information, they are able to use it or even sell the information to others. Before you know it, your debit card balance goes to zero or things you didn't buy show up on your monthly statement.

Online 'data mining' threatens your privacy

It's no secret that Web sites gather information from users. Most of the tracking is through "cookies" that are installed on your computer's hard drive from a Web site you visit. Cookies can contain login information or personalization for a specific Web page.

Using settings on your Web browser, you can control cookies that are placed on your computer, allowing some, allowing none, or even clearing all the stored cookies.

Deleting cookies, however, will not stop the third-party Web tracking done by tracking services and advertising networks. These groups use your online trail to target you for advertisements and Web sites you did not select and may not want to view.

Some consumer advocates say the actions of data brokers who buy and sell the information can leave users' private information in the wrong hands.

The Federal Trade Commission released a preliminary report in December 2010, which recommends a "do not track" feature on Internet browsers so that consumers can choose whether or not to allow tracking of their online searches. The report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers*, is available online at www.FTC.gov. In addition, Congressional hearings were held in Washington, D.C., regarding possible Federal regulations to establish an online privacy bill of rights.

This level of attention is needed, according to the FTC, because advances in technology allow for data collection and sharing that is often invisible to consumers. The report called on the industry to add "do not track" features to Web browsers.

Since then, Google (Chrome 10), Mozilla (Firefox 4), and Microsoft (Internet Explorer 9) have added security features that give users greater control over how they are tracked online.

With or without "do not track" regulations, there are some measures consumers can take to manage their personal information and how they are tracked online. First, use a Web browser that allows you to opt out from accepting tracking cookies. Second, before agreeing to any services, read the Web site's privacy policy. Is the service or access to the site worth the loss of privacy you could experience under its terms? For tips on how to read and understand a Web site's privacy policy, visit the Web site of the California Office of Privacy Protection, www.privacy.ca.gov, and click on "Online Privacy."

HOW TO PROTECT YOURSELF

:: DECIDE IF THE CONVENIENCE OF USING A RFID CARD IS WORTH THE RISK OF IDENTITY THEFT.

:: IF NOT, CUT IT UP AND REQUEST A NEW CARD WITHOUT THE RFID CHIP.

:: PURCHASE A SPECIALLY DESIGNED CARD HOLDER, SLEEVE, OR WALLET THAT BLOCKS TRANSMISSION OF RFID INFORMATION.

:: LIKE ANY OTHER CREDIT OR DEBIT CARD, CAREFULLY CHECK YOUR MONTHLY STATEMENTS TO BE SURE ALL OF THE CHARGES ARE YOURS.

lookout for SKY-ROCKETING BANK FEES

IF YOU HAVEN'T CHECKED your bank or credit union statements lately, you probably should. Despite new government regulations on fees, banks and credit unions are finding ways to increase their revenue. According to the Federal Deposit Insurance Corporation (FDIC), fees account for 56 percent of all bank income. Ten years ago it was three percent. Last year, banks collected $37.8 billion in service charges on accounts.

Don't be surprised to find some of these charges on your statement:

» A $2 charge to check your account balance.
» A $6 charge to use another bank's or credit union's ATM.
» An $8 monthly service fee on your checking account.
» A $6–$12 "inactivity fee" on your debit card.
» An annual fee on your checking, savings, or debit card account.
» Overdraft fees.
» ATM usage fees.

On top of that, the percentage of people with no-fee checking accounts has dropped from 76 percent to 65 percent. Also, the minimum balance required to earn interest on your checking account has skyrocketed from an average of $511 to $3,883.

Watch out for something called courtesy overdraft protection, too. When your account balance doesn't cover the full amount of either a check you write or a debit charge, your bank will cover the purchase and then charge you a fee of around $35.

In order to minimize or prevent getting charged bank fees, consumer advocates suggest the following:

» Read your monthly bank statement and challenge inappropriate charges. Make the bank prove these fees are in your contract.
» Avoid using "courtesy overdraft protection" services. Instead, use traditional overdraft protection from a line of credit or your savings account.
» Shop around and compare bank services in order to find one you feel is offering quality services with appropriate fees.
» Be sure to read the contract and understand how bank fees work. Don't take the word of a bank representative.

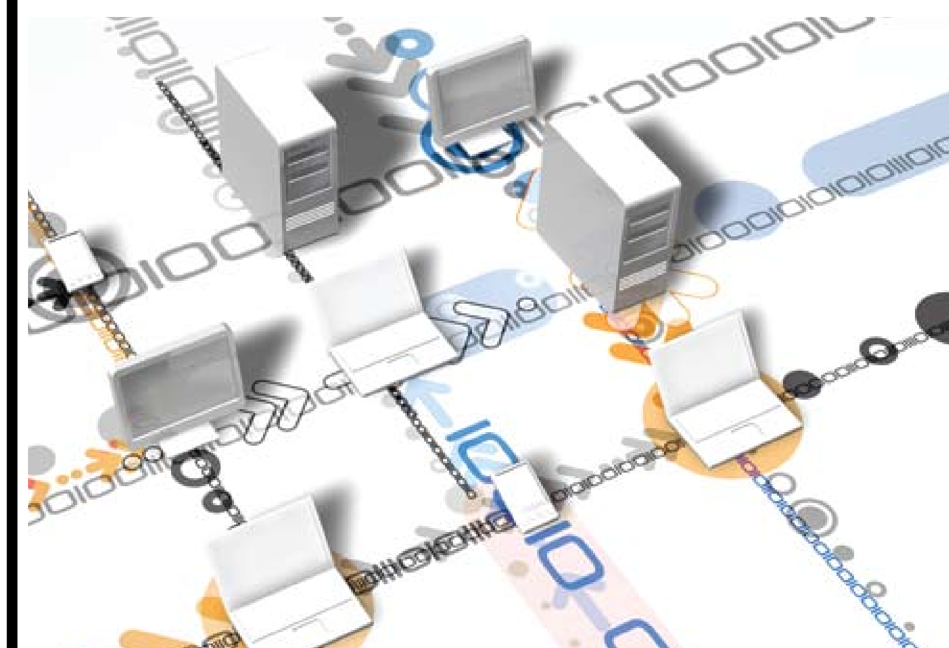
Get into the habit of reviewing your statements each month. Look for fees and charges you feel are wrong and contact your financial institution as soon as a charge appears on your statement for the best chance to get it removed or reversed. Also consider switching to another bank that offers better services, products, and prices.

WATCH OUT FOR WI-FI THIEVES

More than ever, the laptop leaves the house when we do. With Wi-Fi access, it's a great way to check e-mail, verify bank account balances, and do some shopping. Unfortunately, places where Wi-Fi connections are available, such as hotels, airports, and coffee shops, are where the scam artists are, too. They'll try to trick you into connecting to their Wi-Fi router and then steal your personal information. Most people are unaware it's happening until it's too late.

HOW the scam works

You turn on your laptop in a Wi-Fi zone. Several connection choices appear. The problem is some of the connection choices aren't legitimate. These are called ad hoc, or peer–to–peer networks set up by a thief with a laptop and wireless network residing nearby. If you inadvertently connect to their network, all your computer keystrokes will pass directly into their computer. While you're happily surfing the Internet, the hacker is collecting your personal information that can be used to gain access to your bank accounts and credit card numbers.



HOW can you be sure you connect to a legitimate Wi-Fi zone?

Sometimes it's difficult to tell, especially when the scammers model their ad hoc or peer-to-peer network to look exactly like a legitimate one. First, look at your connection page because every network connection includes a name and a description. If it's an ad hoc network, it will be called a "computer-to-computer" network and display an icon of several computers connected together. Do not connect to this.

A legitimate wireless network is simply called a "wireless network." It will display an icon of just one connected computer. This is the legitimate connection.

If you're not sure the Wi-Fi network is legitimate, don't connect. Also, be sure to set up your computer so it doesn't automatically connect to a wireless network but allows you to choose your connection. Always be alert when you're in a Wi-Fi zone and be sure to connect to a legitimate Wi-Fi service provider. Keeping your personal information "personal" depends on it.

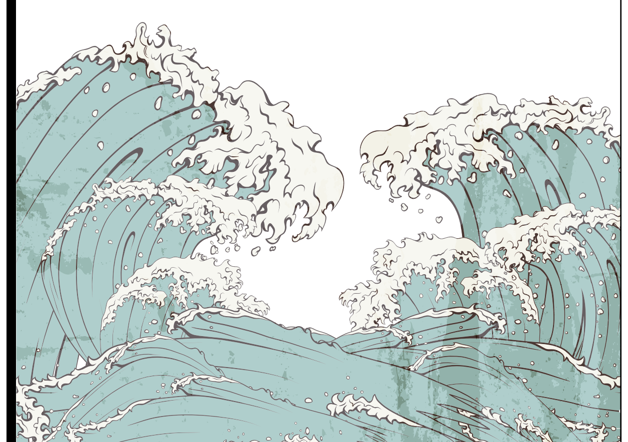
HELP TSUNAMI VICTIMS, BUT AVOID SCAMS

The California Office of the Attorney General is warning Californians who want to help victims of Japan's tsunami to beware of bogus charities.

Here are some tips from the Attorney General on how to give wisely to help disaster relief efforts:

- Carefully review disaster-relief appeals before giving. In times of disaster, many "sound-alike" organizations and sham operations solicit donations.
- Make sure the charity is registered in the Attorney General's Registry of Charitable Trusts. Registration does not guarantee that a charity is effective, but it is an important indicator. A searchable online database is available at ag.ca.gov/charities.php.
- Avoid donating through e-mail solicitations. Clicking on an e-mail may lead you to a Web site that looks authentic but is established by identity thieves seeking to obtain money or personal information.
- Provide your credit card number only after you have reviewed all information from a charity and verified its credibility. Ask the organization not to store your credit card information.
- Do not give cash. Write checks payable to the charitable organization, not a solicitor.
- Take action on your own rather than responding to solicitations. Seek out known, reputable organizations and give directly.

Californians who believe they or others have been victimized by fraudulent charitable solicitations can file a complaint online with the Attorney General's Registry of Charitable Trusts.



OTHER RESOURCES

Better Business Bureau's Wise Giving Alliance
Information on national charities
800.575.4483
WWW.GIVE.ORG

Charity Navigator
Independent charity evaluator, also has guidance on how to help victims of Japan's earthquake and tsunami
WWW.CHARITYNAVIGATOR.ORG

creating a STRONG PASSWORD

HOW MANY different passwords do you have? Too many, right? And trying to remember which password for which Web site you visit? Ugh!

Most of us create passwords that include our name, initials, street address, birthday, anniversary, and pet names. Unfortunately these are considered weak passwords and can be easily hacked. Instead, consider coming up with a "strong" password.

The elements of a strong password are:

» At least one numeric character (0-9)
» At least one lowercase character (a-z)
» At least one uppercase character (A-Z)
» At least one non-alphanumeric character (!,@,#,$,%,&,*)

To create a strong password that will be easy to remember, first come up a phrase that you'll easily remember and then convert the phrase using the first letter (case sensitive) or number in the phrase as part of the password.

For example:

» "I have a 2009 Blue Honda Civic" or Iha09BHC
» "My daughter turns 19 years old in October!" or Mdt19yoiO!
» "Joe Montana won the Super Bowl in 1982" or JMwtSBi82
» "Jim and Sarah got married in July of 1997" or JaSgmiJo97

Be sure your password contains a minimum of eight alpha-numeric characters, as most accounts require one this length. After a little practice, you'll find using this method is both fun and easy. Most importantly, it will be easy to remember and create a more secure environment when using the Internet.

Everyday financial facts to educate and empower

MONEY SMARTS

[IDENTITY THEFT]

Sometimes, consumers are not even aware their identity has been stolen until the thief runs up debts or even commits crimes in your name. Take our little test to see what you know about identity theft. Check the information at the end for some steps you can take to minimize your risk of becoming a victim of this kind of crime.

Identity theft is taking someone else's personal information and using it for financial gain. This kind of crime can take many forms:

- 58 percent involves existing credit card accounts.
- 14 percent involves other existing accounts such as bank accounts and utilities.
- 28 percent involves new accounts and other non-account-related forms of the crime.

In 2009, more than 1 million Californians were victims of identity theft, according to information cited by the California Office of Privacy Protection. For more information about identity theft and what to do if you're a victim of it, visit the Office of Privacy Protection online at www.privacy.ca.gov or call 866.785.9663.

1. WHAT DOES A CON ARTIST DO WITH YOUR STOLEN IDENTITY?
a. Sell your information to other thieves.
b. Take out a loan in your name.
c. Move into your house.

2. WHAT IS A SECURITY FREEZE?
a. A security guard tells you to stop walking.
b. Your bank account is frozen by the court.
c. Credit bureaus restrict access to your credit file, at your request, to prevent anyone from applying for credit in your name.

3. HOW DO YOU PROTECT YOUR PRIVACY?
a. Close the drapes when you're home.
b. Use a fake name in online chat rooms.
c. Shred personal financial documents before you throw them out.

4. IF YOU THINK YOU'VE BEEN A VICTIM OF IDENTITY THEFT, WHAT SHOULD YOU DO?
a. Place a fraud alert on your credit report.
b. Change your name.
c. Switch banks.

5. HOW DO THIEVES GET YOUR IDENTITY INFORMATION?
a. Trick you into giving it to them.
b. Steal your wallet.
c. Call your house and pretend to be from your bank.

6. WHAT IS AN OPT-OUT NOTICE?
a. A written note stating you don't want fries with your burger.
b. A notice that allows you to restrict how your personal financial information is shared by people you do business with.
c. More junk mail.

Answers: 1. a and b; 2. c; 3. c; 4. a; 5. a, b, and c; 6. b

STATE OF CA
DEPARTMENT OF CONSUMER AFFAIRS

Department of Consumer Affairs
Office of Publications, Design & Editing
1625 North Market Boulevard, Suite N-112
Sacramento, CA 95834

PDE 11_017 | 4.2011

CREDIT

OFFICE OF PUBLICATIONS, DESIGN & EDITING

HAZEL ALIG
ARIS BAJAR
JEAN BRICARELLO
LAUREL GODDARD
RAMONA GODOY
ALLEN GRIGG
JIM PYERS
CAROL STOVER
JUNE VARGAS

EDMUND G. BROWN JR.
GOVERNOR

ANNA CABALLERO
SECRETARY, STATE AND CONSUMER SERVICES AGENCY

BRIAN J. STIGER
ACTING DIRECTOR, DEPARTMENT OF CONSUMER AFFAIRS

2009 AWARDS FOR PUBLICATION EXCELLENCE
2009 Winner

GD USA AMERICAN INHOUSE DESIGN AWARD 2008 WINNER
2009 Winner
2008 Winner

NACAA Awards
NATIONAL ASSOCIATION OF CONSUMER AGENCY ADMINISTRATORS
ACE Award 2009
ACE Award 2008

NAGC NATIONAL ASSOCIATION OF GOVERNMENT COMMUNICATORS
2008 Award of Excellence

SIOC STATE INFORMATION OFFICERS COUNCIL
2010 Silver Award
2009 Silver Award
2007 Gold Award